Commonwealth of Massachusetts
Center for Health Information & Analysis (CHIA)
Data Management Plan for Non-Government Entities

DATA MANAGEMENT PLAN

Any Recipients, contractors, or agents receiving CHIA data that includes Protected Health Information ("PHI" as defined under the Health Insurance Portability and Accountability Act [HIPAA] and its implementing regulations) as well as additional elements that may be used to identify an individual (the "Data") must complete and execute this Data Management Plan. The Data Management Plan(s) will be incorporated within the Data Use Agreement that must be executed prior to receipt of the Data. You may wish to refer to the Data Use Agreement as you complete this Data Management Plan. This Data Management Plan should be completed by the Chief Information Security Officer, Chief Privacy Officer, legal counsel or another officer of the organization with sufficient knowledge of the organization's data privacy and security practices and who has authority to bind the organization.

NOTE: This Data Management Plan is confidential and will not become a part of the public record.

I. GENERAL INFORMATION

Project Title: (should appear the same as on the Data Application)	
Recipient Organization: (should appear the same as on the Data Application)	

II. CERTIFICATIONS

The undersigned certifies and agrees as follows:

- The Data will be **encrypted at rest encrypted on storage media (backup tapes, local hard drives, network storage, et al) with at least AES-256 standard or stronger**.
- The Data will **be encrypted in transit consistent with the approved method described in this Data Management plan at section IV.3-b**.
- Anti-virus software or service is active on any server or endpoint containing the Data
- The Organization is in full compliance with the privacy and security requirements of HIPAA
- The Organization has policies and procedures in place to address:
    - The sharing, transmission and distribution of PHI
    - The physical removal, transport and transmission of PHI
    - The physical possession and storage of PHI
    - The training of all staff who will access PHI on the requirements of HIPAA
    - The destruction of PHI upon the completion of its use.
    - Confidentiality agreements will all individuals, including contractors, who will access PHI
    - Business Associate Agreements with all non- employees who will access PHI

Commonwealth of Massachusetts
Center for Health Information & Analysis (CHIA)
Data Management Plan for Non-Government Entities

III. RESPONSIBLE PARTIES

Please identify the following individuals within your organization:

1. The individual responsible for organizing, storing and archiving the Data. This individual is the Custodian of the CHIA Data required under Section 20 of the Data Use Agreement.

Name:	
Organization:	
Title:	
Phone:	
Address:	
Email:	
Reports to (name and title):	

2. The individual(s) responsible for the research team using the Data, including ensuring each individual (i) has a signed confidentiality agreement, (ii) accesses and uses only the minimal Data necessary to achieve the research purpose, (iii) accesses the Data only on a secured server according to Applicant's policies. This individual is also responsible for maintaining the access log required under Section 5 of the Data Use Agreement.

Name:	
Organization	
Title:	
Phone:	
Address:	
Email:	
Reports to (name and title):	

3. The individual responsible for notifying CHIA of any breach of the Data Use Agreement or this Data Management Plan.

Name:	
Organization:	
Title:	
Phone:	
Address:	
Email:	
Reports to (name and title):	

4. The individual responsible for ensuring the Data is destroyed upon termination of the Data Use Agreement, completing the Data Destruction Form and providing that Form to CHIA.

Name:	
Organization:	
Title:	
Phone:	
Address:	
Email:	
Reports to (name and title):	

IV. DATA SECURITY AND INTEGRITY

Complete this section for each location where the Data will be stored or accessed. Any agent or contractor that will have access to or store the CHIA Data at a location other than the Recipient's location, or in an off-site server and/or database, must complete a separate Data Management Plan.

1. *Physical Location of the Data*:

    a. Please provide the delivery address for the Data, as well as the full address, including building and floor, of each location where Data will be stored.

Delivery:

Organization:			
Street Address:	City:	State:	ZIP Code:
Office Telephone *(Include Area Code)*:			

Storage:

Organization:			
Street Address:	City:	State:	ZIP Code:
Office Telephone *(Include Area Code)*:			

i. Will the Data be stored by the third party on a system in the cloud (reachable via the Internet)?
☐ Yes ☐ No

ii. If you answered yes to (a): Has this Cloud Service Provider passed a FedRAMP 3PAO assessment *for the specific cloud system* which will host the data*?*
☐ Yes ☐ No

iii. If you answered yes to (b): What is the name of the provider *and* the FedRAMP level the specific cloud system hosting the data is operating at?

2. *Data Privacy Training and Awareness:*

   a. Has every individual who will access the data received training on the proper handling of protected health information and/or personal data within the last year?
   ☐ Yes ☐ No

3. *Encryption of Data*:

   a. Will all CHIA Data at rest be encrypted on storage media (backup tapes, local hard drives, network storage, et al) with **encryption at least AES-256 or stronger.**
   ☐ Yes ☐ No

b. Will CHIA Data transmitted by your organization over the Internet?
☐ Yes ☐ No

If you answered yes to (b): which of the following if any are used when transmitting data over the internet? If selecting *other* please describe method in space provided below.
☐ SSL (meets or exceeds TSL 1.1 or TSL 1.2) ☐ SFTP ☐ Other

4. *Information Security:*
   a. Does your organization have published information security policies which are followed and accessible to all staff accessing or handling CHIA Data?
   ☐ Yes ☐ No
   b. Has every individual who will access the CHIA Data received cyber security awareness training in the last year?
   ☐ Yes ☐ No
   c. Has your IT organization experienced a breach of PHI or PII in the last seven (7) years?
   ☐ Yes ☐ No

   If you answered yes to (c): how was the breach resolved?

5. *Technical and Physical Controls:*
   a. Are all the user accounts that log on to any machine (server or endpoint) that accesses the Data uniquely assigned to individual users (i.e., the user accounts are not shared)?
   ☐ Yes ☐ No
   b. Is an audit log maintained of all user log-ons to the system hosting the CHIA Data?
   ☐ Yes ☐ No
   c. What is the minimum password length and character complexity (uppercase, lowercase, numeric, and special characters) required for new passwords on the user accounts logging on to the system accessing the CHIA Data?

d. Describe any additional authentication technical security controls you employ to defend the system against unauthorized logon, e.g. maximum failed login attempts, lockout period, etc.:

e. Do you run a current version of a commercial off-the-shelf anti-virus or anti-malware product on the server that will host the CHIA Data?
☐ Yes ☐ No

f. If the CHIA Data will be on a server or network accessible storage drive, then check all the security features present in the room containing CHIA Data:
   i. ☐ Recorded video
   ii. ☐ Access log of all individuals entering the room
   iii. ☐ Secure server rack
   iv. ☐ Access control limiting access only to authorized individuals

g. What additional specific physical or technical safeguards (not mentioned in prior answers) will be used to *mitigate* the risk of unauthorized access to CHIA Data?

h. When was the last information security risk assessment performed in your organization? Who conducted it?

i. When was the last IT audit performed in your organization? Who conducted it?

V. DATA RETURN OR DESTRUCTION

Recipients and contractors are required to attest that the CHIA Data and all copies of the CHIA Data used by the Applicant or its employees, contractors, or agents will be destroyed by the Retention Date as specified in the Data Use Agreement or upon completion of the project described in your Application, whichever occurs first. All data destruction must conform to the requirements of M.G.L. c. 93I and to the Data Use Agreement. Please specify below the technical measures you will use to meet these requirements.

VI. SIGNATORY

The undersigned is an authorized signatory of the organization. The organization hereby agrees to hold and/or access CHIA Data at all times in compliance with all provisions of this Data Management Plan and the Data Use Agreement.

Name:	
Title:	
Organization:	
Signature:	
Date:	